|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Óbudai EgyetemBánki Donát Gépész és Biztonságtechnikai Mérnöki Kar | | | | | | | | | | | | | | | | | Biztonságtudományi és Kibervédelmi Intézet | | | | | | | | | |
| **Tantárgy címe és kódja:** | | | | | | | | **Elektronikus információbiztonság II. BBXEI26BNF** | | | | | | | | | | | | | | | **Kreditérték:** | | | 4 |
| Nappali munkarend | | | | | 3 | | | | | | tanév | | | 1 | | félév | | | | | | | | | | |
| **Szakok melyeken a tárgyat oktatják:** | | | | | | | | | | | | **Biztonságtechnikai mérnök szak** | | | | | | | | | | | | | | |
| **Tantárgyfelelős oktató:** | | | | | | | Dr. habil. Kiss Gábor | | | | | | | | | | | **Oktatók:** | Dr. habil. Kiss Gábor | | | | | | | |
| **Előtanulmányi feltételek (kóddal):** | | | | | | | | | | | | |  | | | | | | | | | | | | | |
| **Heti óraszámok** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Előadás: | 2 | | | | | Tantermi gyak.: | | | | | | | 0 | | | | Laborgyakorlat: | | | | 2 | Konzultáció: | | |  | |
| **Félévzárás módja:** | | | | | | Vizsga | | | | (Válasszon) | | | | | | | | | | | | | | | | |
| ***Online konzultáció*** *(amennyiben szükséges):* | | | | | | | | | | | | | | | *… (BBB link)* | | | | | | | | | | | |
| **Oktatási cél**: | | | *A tantárgy oktatásának célja, hogy a hallgatók megismerjék az operációsrendszerek, online adatbázisok és elektronikus hálózatok információbiztonsági elméletét és gyakorlatát, betekintést nyerjenek a sérülékenység vizsgálati alapelvek gyakorlati alkalmazásának lehetőségeire. A félév során lehetőség nyílik céglátogatásra, ahol az adott cég által használt megoldások kerülnek bemutatásra....* | | | | | | | | | | | | | | | | | | | | | | | |
| **Ütemezés** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Oktatási hét | | **Témakörök** | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. | | Webes adatbázisok felépítése, elméleti alapok. Adatok védelmi lehetőségei (MD5, SHA formátumú adatmentés). | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. | | Social Engineering technikák, a Social Engineering eredményének felhasználása. | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. | | Jelszavak biztonsága, sózás. | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. | | Incidenskezelés tesztelése. Külső sérülékenység vizsgálati módszerek. | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. | | Web sérülékenység vizsgálati módszerek. | | | | | | | | | | | | | | | | | | | | | | | | |
| 6. | | Keyloggerek típusai, Cross Site Scripting. | | | | | | | | | | | | | | | | | | | | | | | | |
| 7. | | 1. Zh. | | | | | | | | | | | | | | | | | | | | | | | | |
| 8. | | Dos, DDoS támadások és az ellenük való védekezési lehetőségek. | | | | | | | | | | | | | | | | | | | | | | | | |
| 9. | | Routeren futó szoftveres védelmi lehetőségek. | | | | | | | | | | | | | | | | | | | | | | | | |
| 10. | | IPS/IDS rendszerek | | | | | | | | | | | | | | | | | | | | | | | | |
| 11. | | SIEM rendszerek | | | | | | | | | | | | | | | | | | | | | | | | |
| 12. | | Layer 2 szinten elvégezhető támadások | | | | | | | | | | | | | | | | | | | | | | | | |
| 13. | | Esettanulmány/céglátogatás | | | | | | | | | | | | | | | | | | | | | | | | |
| 14. | | 2. Zh. | | | | | | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | **Labor témakörei** | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. | | MySQL adatbázistervezés | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. | | MySQL titkosított adattárolási lehetőségei | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. | | Titkosított adatok visszafejtési lehetőségei | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. | | Számítógépes hálózat szegmentálása switch | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. | | Számítógépes hálózat szegmentálása, router | | | | | | | | | | | | | | | | | | | | | | | | |
| 6. | | Számítógépes hálózat szegmentálása, VLAN biztonsági funkciója | | | | | | | | | | | | | | | | | | | | | | | | |
| 7. | | Proxi szerver, mint biztonsági elem | | | | | | | | | | | | | | | | | | | | | | | | |
| 8. | | DMZ, mint biztonsági terület | | | | | | | | | | | | | | | | | | | | | | | | |
| 9. | | PAT, mint hálózatvédelmi eszköz | | | | | | | | | | | | | | | | | | | | | | | | |
| 10. | | NAT, mint hálózatvédelmi eszköz | | | | | | | | | | | | | | | | | | | | | | | | |
| 11. | | SSH védelem | | | | | | | | | | | | | | | | | | | | | | | | |
| 12. | | SSL/TLS | | | | | | | | | | | | | | | | | | | | | | | | |
| 13. | | Esettanulmány/céglátogatás | | | | | | | | | | | | | | | | | | | | | | | | |
| 14. | | Összefoglalás | | | | | | | | | | | | | | | | | | | | | | | | |
| **Félévközi követelmények** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Zárthelyi dolgozat. | | | | | | | | | Beadandó feladat | | | | | | | | | | | Labormérés | | | | | | |
| száma | | | | időpontok | | | | | száma | | | | | | | | határidők | | | száma | | | | időpontok | | |
| 2 db | | | | félév elején egyeztetve | | | | | db | | | | | | | |  | | | db | | | |  | | |
| **Az értékelés, a lebonyolítás, a pótlás módja, a jegy kialakításának szempontjai**  *Értékelés: Az aláírás megszerzésének feltétele az évközi zárthelyik legalább elégséges szintre való teljesítése.*  *Elégséges>40%*  *Közepes>55%*  *Jó>70%*  *Jeles>85%*  *Zárthelyi dolgozatíráskor, ill. vizsgán a meg nem engedett segédeszközök (puska, mobiltelefon, stb.) használata, ill. arra tett kísérlet, továbbá bármilyen információcserére tett kísérlet az érintett hallgató(k) letiltását vonja maga után.*  *A szorgalmi időszak utolsó hetében lehetőség van a sikertelen, illetve igazoltan (pl. betegség) mulasztott zh-k pótlására.*  *Az évközi jegy/aláírás szorgalmi időszakon túli pótlásának módja: HKR 47. §*  *Hiányzás szabályozása: HKR 46. §*  *Valamennyi, jelen dokumentumban nem szabályozott, kérdésben az Óbudai Egyetem Hallgatói Követelményrendszere, valamint Tanulmányi Ügyrendjének rendelkezései az irányadók.* | | | | | | | | | | | | | | | | | | | | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Letiltva bejegyzést kap:** | | | Aki eléri, illetve meghaladja a megengedett hiányzások számát, illetve egyik zárthelyi dolgozatot sem írta meg és nem igazolta megfelelően a hiányzását (pl. betegség esetén orvosi naplószámot tartalmazó igazolással). | |
| **Kötelező irodalom:** | | Előadás jegyzet | | |
| **Ajánlott irodalom:** | Georgia Weidman: Penetration Testing: A Hands-On Introduction to Hacking, ISBN: 978-1593275648, 2015 | | | |
| **A tárgy minőségbiztosítási módszerei:** | | | |  |

Kelt: Budapest, 2023. 06. 15.

Szöveg beírásához kattintson vagy koppintson ide.

………………………………………………………

Dr. habil. Kiss Gábor